BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-223

27 DECEMBER 2002

Communications and Information

IDENTIFICATION AND AUTHENTICATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/WFPS (MSgt Vincent Jones)

Certified by: HQ USAF/XICI
(Col Linda K. McMahon)

Supersedes AFMAN 33-223, 1 June 1998

Pages: 18
Distribution: F

This Air Force manual (AFMAN) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*); Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; and *Computer Security Act of 1987* (Public Law [P.L.] 100-235). It relates to Air Force Instruction (AFI) 33-202, *Computer Security* and DoD Chief Information Officer Guidance and Policy Memorandum 6-8510, Department of Defense Global Information Grid Information Assurance. It provides identification and authentication computer security requirements for all information systems (e.g. voice, video, data, imagery, and sensory). This manual applies to all Air Force military, civilian (to include summer hires and volunteers), and contractor personnel under contract by DoD, who use information systems. Additional security instructions and manuals are listed on the Air Force website at Uniform Resource Locator (URL): **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this manual through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication.** Provide an information copy to HQ AFCA/WFP, 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. See **Attachment 1** for a glossary of references and supporting information. Maintain and dispose of records created as a result of prescribed processes according to AFMAN 37-139, *Records Disposition Schedule*. Public Law 104-12, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Forms Management Program*, affect this publication.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Changes to this document update policy, procedures, and responsibilities to include the system owner and developer, strengthens minimally acceptable password criteria, and mandates that all passwords passing through the installation security boundary must be protected. This document further mandates what events must be audited in every information system and how long those audit records must be maintained. **Chapter 1** updated. Paragraph **1.1.** changed term Computer System Security Officer (CSSO) to Information System Security Officer (ISSO), and all references throughout the document. Purpose reworded--updated. Added information on system security authorization agreement (SSAA) requirements. Expanded (paragraph **1.4.**) "Responsibility" paragraph to include DAA and functional system owners. **Chapter 2** swapped with **Chapter 3**. Initial assignment updated to reflect new requirements that are now defined in AFI 33-115 Volume 2, *Licensing Network Users and Certifying Network Professionals*, (versus AFI 33-204, *Information Assurance [IA] Awareness Program*). Removed reference to password attachment. Expanded password aging and management, and user-id uniqueness section. **Chapter 3** information moved to **Chapter 4**. References governing password classification updated. Password transmission and multiple account section were both expanded. Added password storage section. **Chapter 4** information moved to **Chapter 5**. Modified "maintaining user accounts" section to delete/disable accounts inactive for 120 days. Modified "system configuration" section, calling for inactive workstations to be automatically logged off after 8 hours of inactivity. Updated audit trail references to AFI 33-202. Reduced "Security tools" section; specific references to individual tools replaced with statement explaining who is authorized to use such tools and where authorized tools can be found. Added paragraph **5.8.** "information collection, records, and forms" section; provides instructions on proper maintenance and storage of information.

Chapter 1

GENERAL INFORMATION

1.1. Purpose. This manual provides information system owners, developers, system users, system administrators, workgroup managers, and Information Systems Security Officers (ISSO) with the minimum identification and authentication (I&A) techniques and procedures. System owners and developers must design systems that are compliant with the policy contained in this publication. "Identification" is the process where individuals or network devices are identified to a system as a valid user. "Authentication" is the procedure where the system verifies the individual or network device has a right to access the system or system resources. The most common I&A method is a username and password pair because this is the default provided by the most commonly used computer operating systems. The default implementations are weak in several aspects resulting in one of the most common vulnerabilities. This manual provides information and guidance on alternative, stronger methods and how to reduce the risks of using the default method.

1.2. Applicability. This manual applies to all Air Force information systems that must employ I&A techniques and supports the individual accountability requirement established in AFI 33-202. **If there is a conflict between this AFMAN and another more specialized document, the more specialized document takes precedence (i.e., documents governing Sensitive Compartmented Information systems).** Specific criteria established in this AFMAN not incorporated due to technical, procedural, or feasibility constraints must be identified in the system certification and accreditation documentation, the system security authorization agreement (SSAA). Before fielding a system that is noncompliant with the I&A criteria established in this manual, the system must first be approved by an Air Force or MAJCOM Chief Information Officer's issuance of a Certificate of Networthiness and the residual risk and liability must be accepted by the system's Designated Approving Authority (DAA).

1.3. Relationship to Other Publications:

1.3.1. AFI 33-202 defines the password as a method of authentication to support accountability and access control.

1.3.2. CSC-STD-002-85, *Department of Defense Password Management Guideline*, provides a set of practices related to using password-based user authentication mechanisms.

1.3.3. NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems*, provides guidance on designing and incorporating effective identification and authentication mechanisms.

1.3.4. Federal Information Processing Standards (FIPS) Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*, discusses techniques for the identification of individuals for the purpose of controlling access to computer networks.

1.3.5. FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, provides information and guidance on techniques and practices used to control access to computer resources via remote terminals and networks.

1.3.6. FIPS Publication 112, *Password Usage*, defines 10 factors to be considered in design, implementation, and use of access control systems that are based on passwords. It specifies minimum-security criteria for such systems and provides guidance for selecting additional criteria for password systems that must meet higher security requirements.

1.3.7. FIPS Publication 181, *Automated Password Generator (APG),* specifies the standard to be used by Federal organizations that require computer generated pronounceable passwords to authenticate the personal identity of an information system user, and to authorize access to system resources. The standard describes an automated password algorithm that randomly creates simple pronounceable syllables as passwords.

1.3.8. FIPS Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, describes the primary alternative methods for verifying the identity of information system users and provides recommendations to Federal agencies and departments for the acquisition and use of technology that supports these methods.

1.3.9. FIPS Publication 196, *Entity Authentication Using Public Key Cryptography*, specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These protocols may be used during session initiation, and any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

1.3.10. Air Force Chief Information Officer (AF-CIO) Memorandum, *AF Public Key Infrastructure (AF PKI) Guidance*, 29 March 1999 states the requirement for systems to use AF PKI Certificates for identification and authentication to unclassified networks and private web servers. AFI 33-213, *DoD Public Key Infrastructure Management and Use* will replace this memorandum.

1.4. Responsibility. Functional system owners, DAAs, and system developers are responsible for ensuring the I&A criteria established in this manual are incorporated and then maintained in each system throughout its life cycle. System administrators or workgroup managers are responsible for maintaining the I&A management program for the system; creating, distributing, controlling, and deleting identifiers and passwords; and adhering to the criteria outlined in this manual. Assign ISSOs to assist system administrators in I&A management according to AFI 33-202.

Chapter 2

METHODS OF IDENTIFICATION AND AUTHENTICATION

2.1. Introduction . Usernames and passwords are only one method available to identify and authenticate a user's identity. Passwords are popular because of their low cost; however, poor password use and management have left many systems vulnerable and are a common reason in the majority of system penetrations. This has encouraged the continued pursuit of more reliable methods. When necessary and appropriate, use other I&A methods as well.

2.2. Knowledge-Based . Knowledge-based I&A systems require the user to provide a pre-established piece of information in order to gain access. The authentication succeeds if the information provided by the user matches what the system expects. This approach is based on the concept that the user is the only one who knows what the information system expects and therefore is the person identified. This technique is vulnerable to attack by guessing or deducing the information. If the information is too simple or too easily associated with the person, it is more susceptible to hacker penetration. Examples of knowledge-based I&A include passwords, personal identification numbers (PIN), and other personal data. The user provides a unique piece of identification to the system; the system then prompts the user for that unique piece of information as an authenticator. This is by far the most common method used today to access an information system.

2.3. Possession-Based . Possession-based I&A systems require the user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain information physically, magnetically, or electrically coded in a form recognized by the host system. These systems reduce the threat from perpetrators who attempt to guess or steal passwords, because the perpetrator must either fabricate a counterfeit token or steal a valid token from a user. Examples of this technique include physical and electronic keys, challenge-response generators, smart cards (FORTEZZA or FORTEZZA PLUS), public key infrastructure (PKI) supported common access cards/software tokens) or badges. PKI is the vehicle used to facilitate certificate (common access card) generation and revocation, and certificate management services.

2.3.1. Public Key Infrastructure (PKI). Includes a combination of hardware, software, policies, and procedures as well as the ability to authenticate, protect, and digitally sign electronic mail and documents. DoD is implementing PKI to ensure that information is transmitted securely across the internet and all military networks and has directed that all web servers are secured and e-mails are digitally signed. Digital signatures are as legally binding as handwritten signatures.

2.3.2. Common Access Card (CAC). CAC is the new DoD identification card. It is a credit card-sized ID card that contains integrated circuit chips, magnetic strip, bar codes, and photo ID. The integrated circuit chip is where your PKI certificate/keys will reside. You will use your CAC to digitally sign e-mail and other documents and establish secure e-mail sessions.

2.4. Biometric-Based . Biometric-based I&A systems rely on a unique physical characteristic to verify the identity of a user. Common identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. These authentication devices tend to cost more than knowledge- or possession-based systems, because the hardware required to capture and analyze physical characteristics is more complicated. However, these systems provide a very high level of security because the authentication is directly related to a user's unique physical characteristics that are more difficult to counterfeit.

2.5. Combining Methods . One method that can substantially increase the security of an I&A system is to use a combination of I&A techniques. These techniques make it much more difficult for the perpetrator to obtain the necessary items for access. Automated teller machines have the most widespread use of this technique. The user must have a legitimate card with the correct information contained on the magnetic strip as well as a PIN. Even if a perpetrator gets the card, they would need to guess or determine the PIN. This is why users are warned not to keep the PIN stored with the card.

2.6. Strong Authentication . Combination of two of the above methods constitutes strong user authentication as does cryptographically protected authentication (encrypted) or one-time passwords.

Chapter 3

IDENTIFICATION AND AUTHENTICATION ISSUANCE PROCEDURES

3.1. Introduction. System owners and developers must adhere to the specifications contained in this chapter when designing or modifying their system that uses usernames and passwords for identification and authentication. System administrators follow procedures contained in this chapter when creating and managing information system accounts and passwords.

3.2. Initial Assignment. Prior to issuing usernames and passwords, make sure the user possesses a valid license to access the network according to guidance contained in AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*. Make sure the user is briefed on the importance of protecting their username and password; password construction, aging and reuse; reporting any suspicious activity, fraud, waste, and abuse; and the use of system monitoring.

3.2.1. Organizations make sure a method is in place to authenticate requests for information system access before issuing passwords.

3.2.2. DAAs may require formal documentation for classified system requests. Use National Security Agency (NSA) Form G6521, **Access Request and Verification**, National Stock Number 7540-FM-001-34482; Defense Information Systems Agency (DISA) Form 41, **System Authorization Access Request**, or a MAJCOM or locally prescribed form/letter.

3.3. Password Generation. Use passwords generated by the information system or require users to generate their own password.

3.3.1. Adhere to requirements in CSC-STD-002-85 to meet an acceptable information system-generated password algorithm. Passwords generated by the information system must meet the criteria outlined in this publication.

3.3.2. Passwords generated manually by the user must meet the criteria outlined in this publication.

3.4. Password Composition:

3.4.1. Each password must contain a minimum of eight characters comprised of at least one uppercase character, one lowercase character, one number, and one special character (@&+, etc.).

3.4.1.1. Modify systems unable to support eight character passwords or other composition requirements at the earliest and most cost-effective opportunity. In the interim, use the maximum number of characters and composition requirements the system is capable of supporting.

3.4.2. **Attachment 2** provides tips for effective password composition. Never make a password related to one's own personal identity, history, or environment.

3.4.3. Passwords will not contain dictionary words spelled frontward, backward, or split with a number or special character.

3.4.4. Passwords will not contain the username or the user-ID.

3.5. Generic Passwords. Generic password assignment is prohibited (e.g., a system having "welcome" as the password for all newly created accounts) unless the user is required to change the password upon initial log-in. In this case, disable user accounts until the user is immediately ready to log in for the first time.

3.6. Password Aging and Management. Change passwords at a minimum of every 90 days on those systems compliant with the policy set out in paragraph 3.4. Establish a more frequent policy for systems not in compliance with the policy in paragraph 3.4. Document the frequency in the SSAA.

3.6.1. Establish a minimum amount of time that must elapse before a user may optionally change their password. The default minimum before a password can be changed is 5 days.

3.6.2. Users must be deterred from using former passwords. Depending upon system capabilities, this can be done by implementing a minimum 6-month password age or by preventing the reuse of the current password and the last nine passwords.

3.6.3. Limit the number of attempts allowed for correct password entry. Set the degree of password entry protection and the number of allowed entry attempts according to the sensitivity of the protected data. The default permits a maximum of three attempts. This will defeat the brute force password attack of repeatedly entering a password.

3.6.3.1. When the maximum number of password attempts is exceeded lock out the user account or terminal from use. Make sure procedures are in place so the user's identity is first authenticated through the system administrator or the workgroup manager before the account is unlocked. Make sure a user cannot defeat this procedure.

3.6.3.2. Be aware that this policy can be used to cause a denial of service by locking out all user accounts or terminals. DAAs are to use operational risk management to determine which vulnerability, brute force password attack or denial of service attack, causes the biggest threat to their system. If denial of service is the bigger threat, the DAA can authorize that lockout mechanism be based on time delay before being reactivated. The minimum time recommended is 24 hours before automatic reactivation.

3.7. Username Uniqueness. To enforce individual accountability uniquely identify each user within a system. Do not reissue a username to another person for 1 year after its previous deletion.

3.7.1. All users must uniquely identify themselves before beginning to perform any actions that the system is expected to accomplish.

3.7.1.1. Each user must log into his individual unique account to assume a trusted profile (e.g., system administrator, security officer, root user, super user).

3.7.1.2. On systems with a high user turnover, such as in a training organization, the system administrator may substitute reusable generic usernames ($tuDent1, $tuDent2, c@Det001, c@Det002, etc.) for user unique IDs. In this case, the system administrator must incorporate a tracking method to match individual students to generic usernames (e.g., user log sheet, etc.). Once the student no longer requires access (new module, class graduation, etc.), cancel the passwords associated with the user names.

3.7.2. Each user must be uniquely identifiable (e.g., username or user-ID) within the Air Force Global administrative domain.

3.7.3. Each system must provide the capability of associating the user's identity with all auditable actions taken by that individual.

3.7.4. Occasionally, concerns about mission accomplishment necessitate using group usernames and passwords. System administrators allowing group accounts and passwords must maintain individual accountability. A manual solution is to require account users to note access date and time on a log sheet. The process must be fully documented in the SSAA and the risk must be accepted by the DAA.

Chapter 4

PROTECTION PROCEDURES FOR PASSWORD-BASED IDENTIFICATION AND AUTHENTICATION SYSTEMS

4.1. Introduction. Follow the policy contained in this chapter to control password disclosure.

4.2. Password Protection. Each user is responsible and accountable for their own password.

4.2.1. Memorize your password. Do not place passwords on desks, walls, sides of terminals, or store them in a function key, log-in script, batch file, or the communications software (i.e., do not save password on log-in scripts). If documentation is necessary for mission accomplishment (i.e., preestablished accounts for contingency or exercise), place the password in a properly marked, sealed envelope and store it in a safe. In the case of web-based log-in, the fact that an individual user has authenticated can be tracked for that session only (i.e., through the use of nonpersistent cookies or preferences) but the actual password used cannot be stored or passed on.

4.2.2. Each user must enter his username and password upon initial access to an information system. A user must enter a password in such a manner that the password is not revealed to anyone observing the entry process.

4.2.3. Do not share your password. If password sharing is necessary for mission accomplishment make sure the password is changed immediately after shared access is no longer required.

4.3. Password Classification. Protect all passwords based on the sensitivity of the information or critical operations they protect (i.e., a password used to gain access to a SECRET network is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only" (FOUO). See Chapter 4 of DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*, for an explanation of FOUO. Usernames are an unclassified reference to a user that can be displayed on printouts and in audit trails without compromising the password.

4.4. Password Transmission. During transmission, protect passwords at the same level required for the system or data that the password is protecting. Passwords are typically sent for authentication from a terminal to the system by a communications line. Unless the line is afforded the appropriate physical protection (e.g., dedicated point-to-point circuit) or encrypted, the password is vulnerable to disclosure by wiretapping and sniffers. Prevent this vulnerability by electronic protection or password encryption. In general, all passwords should be encrypted/protected. At a minimum, all passwords that pass through the installation's logical security perimeter (e.g., firewall, etc.) must be protected or encrypted according to AFI 33-201, (FOUO) *Communications Security (COMSEC)*, with a minimum of a FIPS 140-2, *Security Requirements for Cryptographic Modules,* validated product. If this is not technically feasible, then alternative nonpolicy compliant encryption may be used as long as the waiver procedures in AFI 33-201 are followed and the waiver is approved. If neither an encryption policy compliant or noncompliant solution is available, then use of a one-time password to access the system or process must be used (i.e., system administrator changes the password after every use.)

4.5. Password Storage. To prevent unauthorized disclosure of passwords while they are stored, password authentication files must not contain clear text authentication data.

4.6. Unattended Workstations. Never leave the information system unprotected while “logged in.” Immediately invoke the system’s password-protected screen saver (if so equipped) or employ physical measures (e.g., keyboard locks) before leaving the information system unattended. If a screen saver or keyboard lock is not installed, the user must log off before leaving the workstation unattended.

4.7. Password Change Authorization. Users may use an established procedure to change their own password whether it is machine or user generated. Prompt the user to enter the old password and authenticate as part of the password change procedure.

4.7.1. If the user forgets the password, the system administrator or workgroup manager must personally verify the user’s identity before changing the password.

4.7.2. If given a generic password (e.g., “Pa$$w0rd”), the system must prompt the user to immediately change to a new password. If the system is incapable of such a function, the system administrator must walk the user through the password change procedure.

4.8. Multiple Accounts. Use one of these four options if users require access to multiple systems:

4.8.1. Option 1: A different username but same password for all systems. (This is the least secure and most risky choice.)

4.8.2. Option 2: The same username but different password for all systems.

4.8.3. Option 3: A different username and different password for all systems. (This is the preferred solution from a security perspective.)

4.8.4. Option 4: Single sign-on as defined in FIPS 190.

Chapter 5

USER ACCOUNT MAINTENANCE AND MANAGEMENT RESPONSIBILITIES FOR PASSWORD-BASED I&A SYSTEMS

5.1. Introduction. System administrators and workgroup managers will follow the policy contained in this chapter.

5.2. Default Accounts. Applications must never require a system administrator account labeled “root” as a requirement to log in to the system, or for an application to run. In addition, anonymous and guest log-ins must not be required for remote access.

5.2.1. Delete all unnecessary accounts and change all factory default or user-generated passwords included in a newly acquired system (software or hardware) before allowing any user access to the system. Many hardware components, such as servers, routers, and other networking devices come from the vendor installed with a few standard usernames (such as SYSTEM, TEST, MASTER, etc.) and passwords.

5.2.2. System owners and developers will not ship a system with active default or hidden maintenance accounts or passwords. If a development system’s default account (not the same as a default manufacturer account) is active when the system is installed, system administrators will disable that account as soon as the system is operational.

5.3. Disabling And Deleting User Accounts and Passwords. Disable and delete all user accounts from an information system whenever the user is permanently transferred to another location or terminates employment.

5.3.1. Ensure procedures are in place so the Network Control Center, workgroup manager, and system administrator are notified when an employee (military, civilian, or contractor) transfers, retires, separates, or is terminated.

5.3.2. If a user is suspended from work, or system access is revoked or suspended for any reason, immediately disable the account and follow guidance in AFI 33-115, Volume 2.

5.3.3. Change a suspected or confirmed compromised password immediately.

5.4. Maintaining User Accounts. Review account usage for systems every 6 months to help identify dormant accounts on the system.

5.4.1. Delete or disable all accounts with inactivity exceeding 120 days. Consider disabling user accounts when they are on an extended TDY and they are unable to remotely access their accounts during the TDY.

5.4.2. Ensure procedures are in place so the user must personally request account reinstatement from the system administrator or workgroup manager. The system administrator or workgroup manager must personally authenticate the user’s identity prior to reinstating an account.

5.5. System Configuration. Design, enable, and configure the following information system features:

5.5.1. Design and configure the system to prevent rapid retries when entering a password incorrectly by allowing several seconds to elapse before requesting another password. This delay deters any automated, high speed, trial-and-error attack on the password system.

5.5.2. Following a successful log-in procedure, inform the user of the last successful access to the account and of any unsuccessful intervening access attempts. This aids in uncovering any unauthorized or attempted accesses that may have occurred.

5.5.2.1. If the system technically supports this capability it must be enabled. If the capability is not supported by the system, document the vulnerability in the SSAA and the risk must be accepted by the DAA.

5.5.3. Automatically log a user off the system (e.g., local area network, web-enabled application) if the workstation is inactive for a period of 8 hours. This forces users to reauthenticate themselves after being logged off a system due to inactivity. If accessing through an authorized remote connection (e.g., dial-in, remote access server), automatically terminate the remote session after 15 minutes of inactivity.

5.6. Audit Trails. System administrators must ensure the system's audit trail function is enabled as directed in AFI 33-202. The audit trail contains a record of successful and unsuccessful log-in attempts, file system modifications, change in privileges, and other data critical to the system's operation and security. The audit trail must not contain unencrypted (clear text) passwords, incorrectly entered passwords, or character strings, since this could expose the password of a legitimate user who mistakenly types the user's name or password. The system may provide certain audit reports (e.g., date and time of last log-in) directly to the user. This allows the user to determine if someone else has used the account. Only authorized personnel, such as the system administrator, have access to the audit trail file.

5.6.1. For each recorded event, at a minimum the audit record must identify the system date and time of the event, username or user-ID, type of event, and the success or failure of the event.

5.6.2. For identification and authentication events, the audit record must identify the origin of the request (e.g., terminal ID, host Internet Protocol address).

5.6.3. All audit records must be maintained for a minimum of 6 months according to AFMAN 37-139.

5.7. Security Tools. To the fullest extent possible, system administrators and network security professionals use security tools to provide the best defense against poor passwords. The constant use of a password policy enforcer and periodic routine use of password cracking tools is mandatory. System administrators and network security professionals are the only personnel authorized to use password cracking tools. Only HQ USAF/XI or Joint Technical Architecture-Air Force (will be replaced by the Infostructure Technology Reference Model

(I-TRM)) tools are authorized for use on Air Force systems or networks.

5.8. Information Collections, Records, and Forms.

5.8.1. Information Collections: No information collections are created by this publication.

5.8.2. Records: Maintain and dispose of records created by this publication according to AFMAN 37-139, Table 33-25, Rule 8.

5.8.3. Forms (Adopted and Prescribed).

5.8.3.1. Adopted Forms: AF Form 847, **Recommendation for Change of Publication**; NSA Form G6521, **Access Request and Verification**; and DISA Form 41, **System Authorization Access Request**.

5.8.3.2. Prescribed Forms: No forms are prescribed by this publication.

LESLIE F. KENNE, Lt Gen, USAF
DCS, Warfighting and Integration

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 100-235, *Computer Security Act of 1987*

Public Law 104-13, *The Paperwork Reduction Act of 1995*

CSC-STD-002-85, *Department of Defense Password Management Guideline*

NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems*

FIPS Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification,* April 1, 1977

FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, September 29, 1980

FIPS Publication 112, *Password Usage,* May 30, 1985

FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001

FIPS Publication 181, *Automated Password Generation (APG)*, October 5, 1993

FIPS Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 28, 1994

FIPS Publication 196, *Entity Authentication Using Public Key Cryptography*, February 18, 1997

OMB Circular A-130, *Management of Federal Information Resources*

DoD-CIO Guidance and Policy Memorandum 6-8510, *Department of Defense Global Information Grid Information Assurance*

DoD 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-201, (FOUO) *Communications Security (COMSEC)*

AFI 33-202, *Computer Security*

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-360, Volume 2, *Forms Management Program*

AFMAN 37-139, *Records Disposition Schedule*

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

CAC—Common Access Card

COMSEC—Communications Security

DAA—Designated Approving Authority

DISA—Defense Information Systems Agency

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

FIPS—Federal Information Processing Standards

FOUO—For Official Use Only

I&A—Identification & Authentication

ISSO—Information Systems Security Officer

I-TRM—Infostructure Technology Reference Model

NSA—National Security Agency

OMB—Office of Management and Budget

PIN—Personal Identification Number

PKI—Public Key Infrastructure

SSAA—System Security Authorization Agreement

USAF—United States Air Force

User-ID—User Identification

Terms

Audit Trail—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. ***NOTE:*** Audit trail may apply to information in an information system, to message routing in a communications system, or to the transfer of COMSEC material.

Authentication—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information.

Designated Approving Authority (DAA)—An official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Identification—Process an information system uses to recognize an entity.

Information—Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in media.

Information System—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Log-in—Procedure used to establish the identity of the user, and the levels of authorization and access permitted.

Password—A protected word or string of characters that identifies or authenticates a user for access to a specific system, data set, file, record, etc.

Username or User Identification (user-ID)—Unique symbol or character string used by an information system to identify a specific user.

Attachment 2

PASSWORD MANAGEMENT QUICK REFERENCE SHEET

A2.1. The "DOs" of Password Management. Do:

A2.1.1. Use a combination of letters (upper and lower case), numbers, and special characters. Password must include at least one of each character type.

A2.1.2. Make the password pronounceable for easy memorization (e.g., consonant-vowel-consonant).

A2.1.3. Use a length of eight or more characters in the password.

A2.1.4. Change your password every 60 to 90 days.

A2.1.5. Protect your password so you are the only one to know it.

A2.1.6. Enter the password carefully making sure nobody is watching.

A2.1.7. Use your account regularly to help you remember your password.

A2.1.8. Contact your ISSO if you suspect your password has been compromised.

A2.1.9. Make sure your password is not exposed on the screen during log-in.

A2.1.10. Verify the log-in information provided to make sure your account has not been used since your last session.

A2.2. The "DON'Ts" of Password Management. Don't:

A2.2.1. Use a single word by itself for the password; especially ones from the dictionary, slang words, names, or profanity.

A2.2.2. Use words personally associated with you.

A2.2.3. Write down your password unless absolutely necessary; if written, protect it so you are the only one who knows it.

A2.2.4. Store your password on the desk, wall, terminal or in a function key or the communications software.

A2.2.5. Share your password with anyone.

A2.2.6. Let anyone watch you enter your password.

A2.2.7. Leave your terminal unprotected while you are logged in.